Amendments to the Specification:

The following amendments are made to the substitute specification filed with the Applicants' immediately prior amendment mailed November 4, 2005.

Please replace paragraph [0042] with the following amended paragraph:

[0042] In FIG. 3, there is shown an advantageous variant of the invention, the key having been loaded with fixed contents of the shift register (which may also consist purely of zeros) and clocking the shift register taking place with an active linear and an active non-linear feedback function, but without data being loaded into the shift register during the [[-]]clocking period. In doing so, the input of data into the shift register after loading the key is disconnected from the shift register and is reinstated again after a specific [[-]]clocking period. Due to the fixed contents of the shift register, it is not permitted to apply any modifications and an unauthorized third party shall not be capable of determining a collection of different values of leak data, such as power consumption, and subject it to statistical analysis in order to retrieve the key.